Introduction to Safety Systems in Research Accelerators

Architectures

USPAS

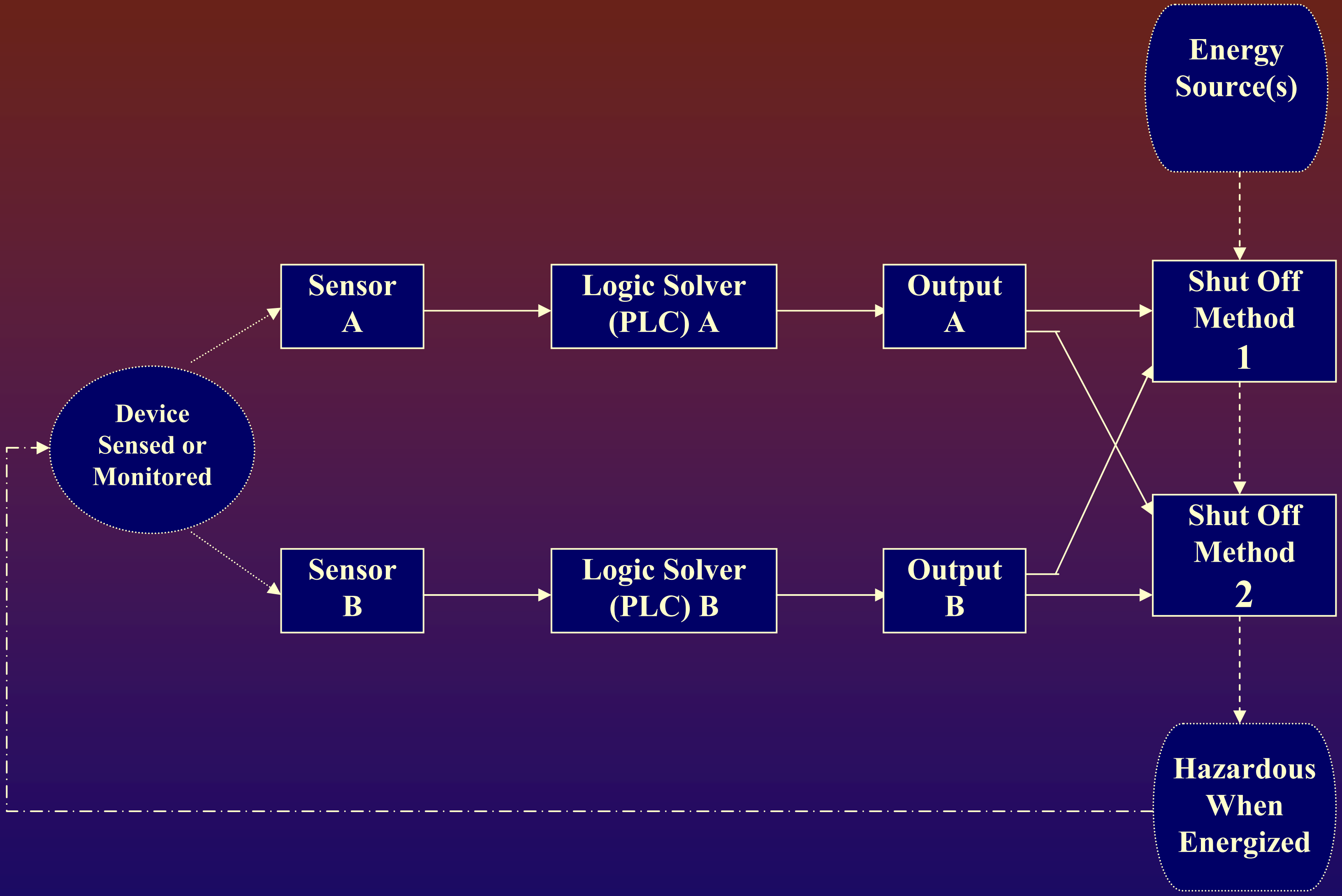
June, 2004

Architectures

- High level implementation of system
- Takes in to account:
  - Final control devices
  - Physical Environment
  - Constraints on physical design
  - R-M-D

RMD – Redundancy Multiplicity Diversity

- **Three elements of the architecture are used to achieve the required safety integrity level**
- **Redundancy** – is the use of identical safety functions to achieve a high safety reliability
- **Multiplicity** - is the use of multiple shutdown paths or protection devices
- **Diversity** – is the use if different types of devices to reduce the probability that multiple or redundant devices can be affected by common failure modes.
-



Energy Source(s)

Sensor A

Logic Solver (PLC) A

Output A

Shut Off Method 1

Device Sensed or Monitored

Sensor B

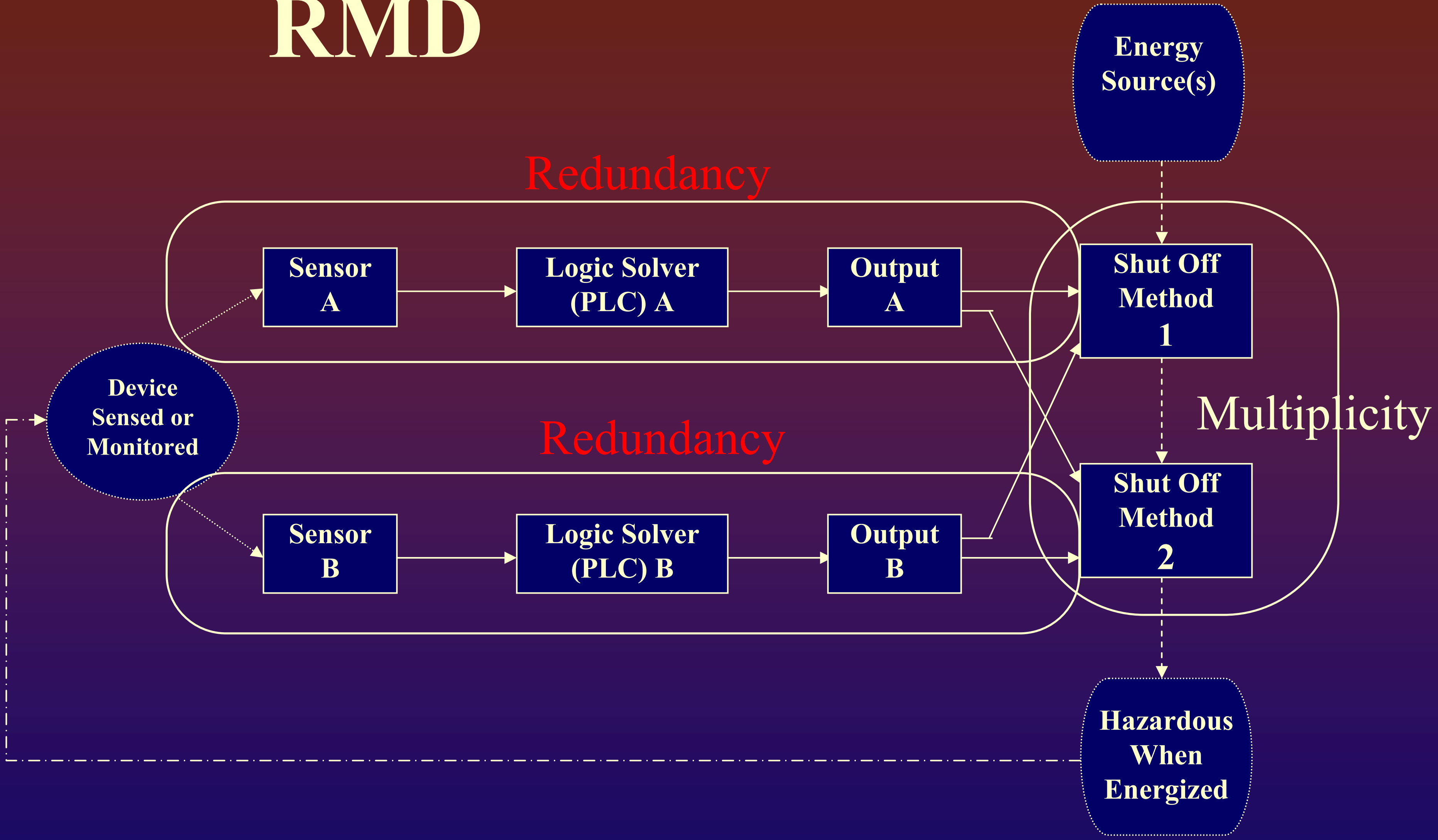
Logic Solver (PLC) B

Output B

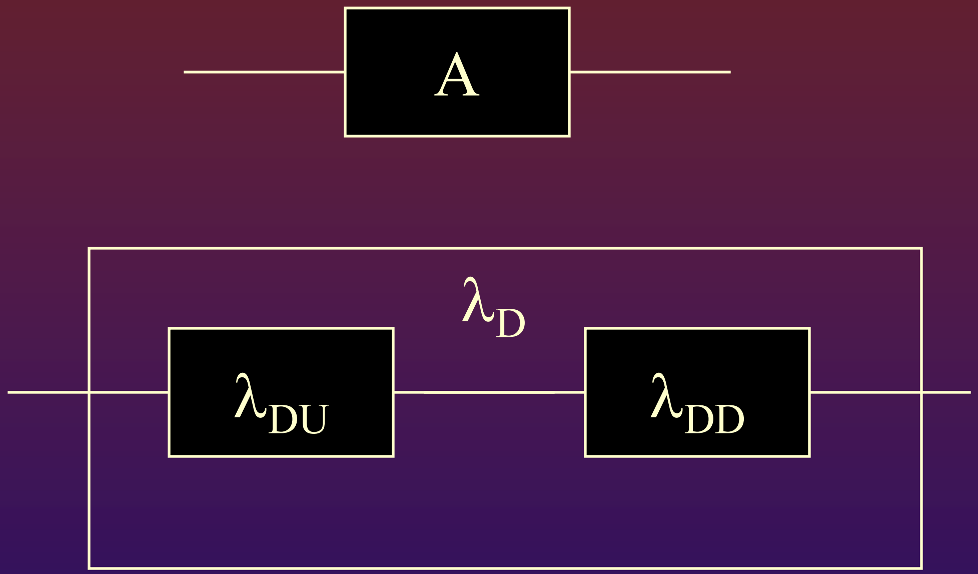
Shut Off Method 2

Hazardous When Energized

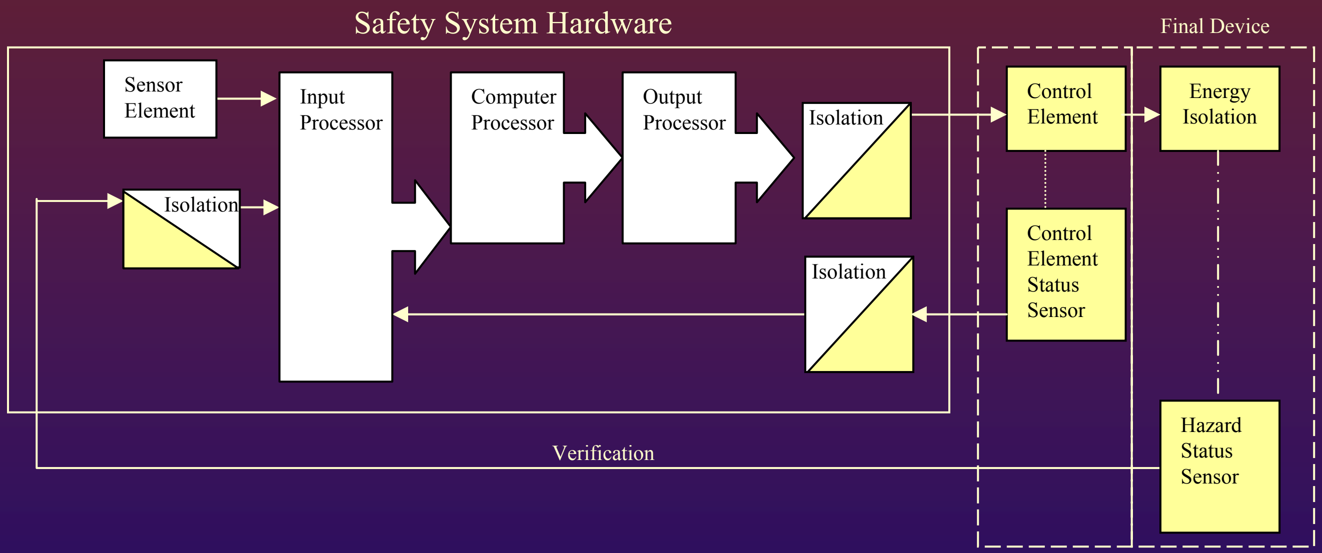
RMD


Energy Source(s)
Redundancy
Sensor A
Logic Solver (PLC) A
Output A
Shut Off Method 1
Device Sensed or Monitored
Multiplicity
Redundancy
Sensor B
Logic Solver (PLC) B
Output B
Shut Off Method 2
Hazardous When Energized

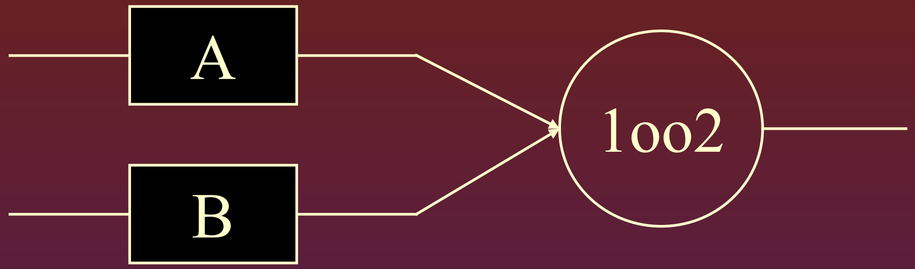
1oo1

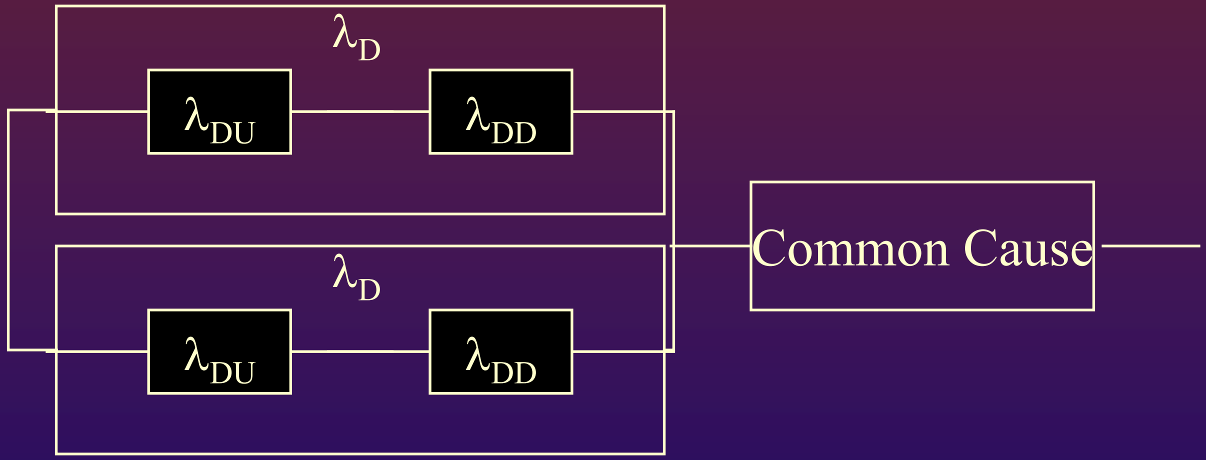


$$\text{PFD} \approx \lambda_D \text{TI}$$


Safety System Hardware
Final Device
Sensor Element
Input Processor
Computer Processor
Output Processor
Isolation
Isolation
Isolation
Control Element
Energy Isolation
Control Element Status Sensor
Hazard Status Sensor
Verification

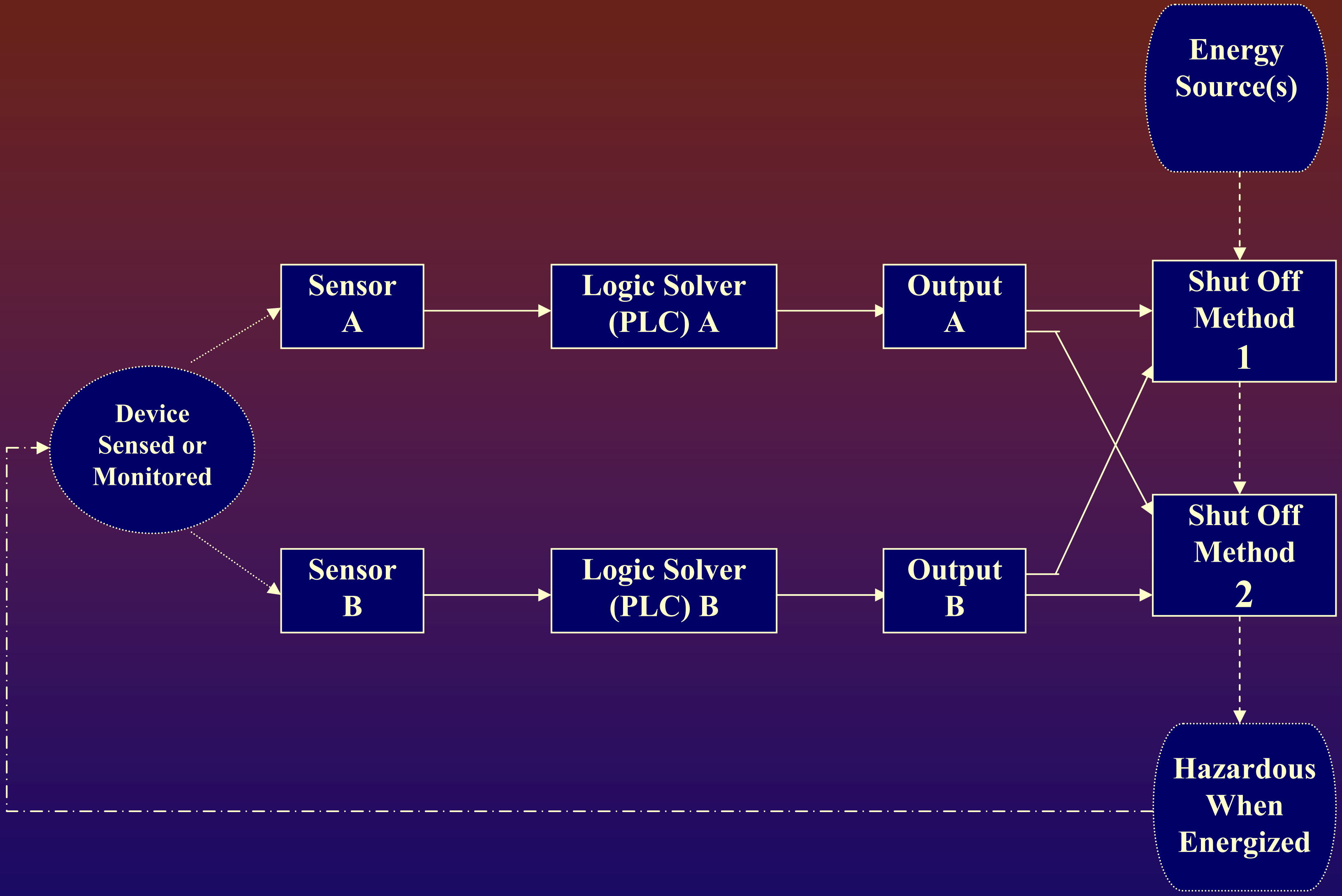
1oo2



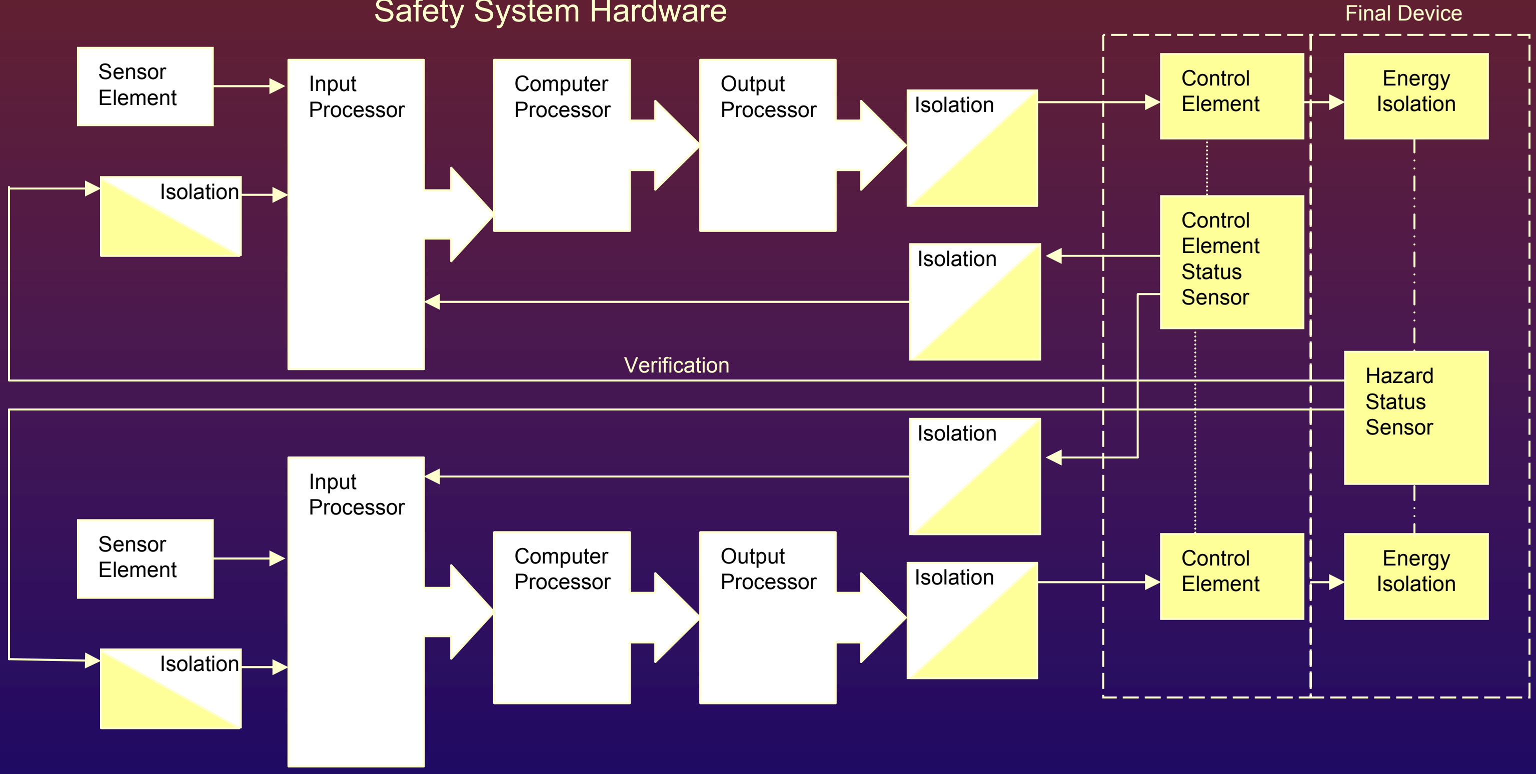


$$PFDavg = 2((1-\beta)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 TI + \beta\lambda_{DD}MTTR + \left(\frac{TI}{2} + MTTR\right)$$

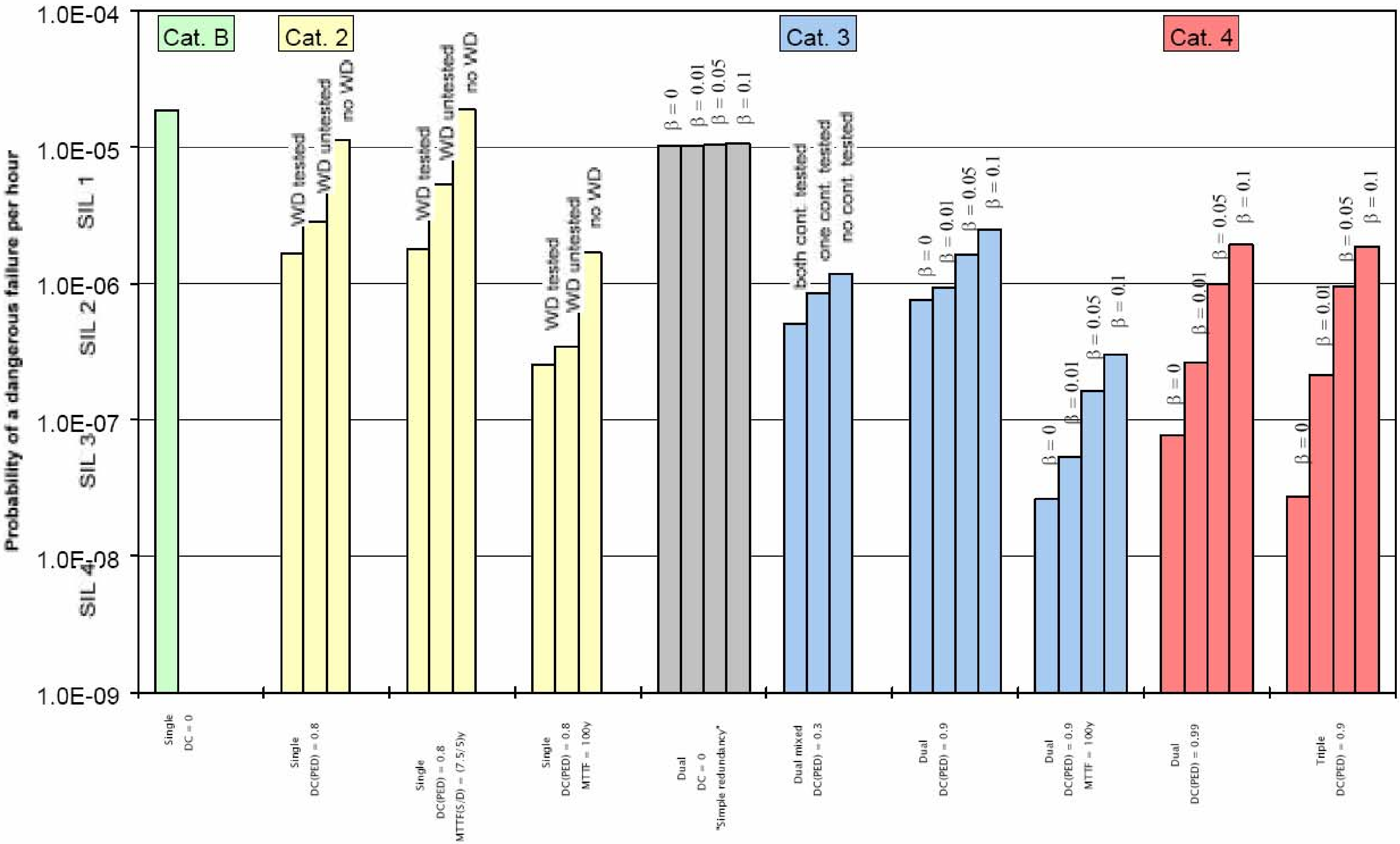
1oo2 Block Diagram



Safety System Hardware

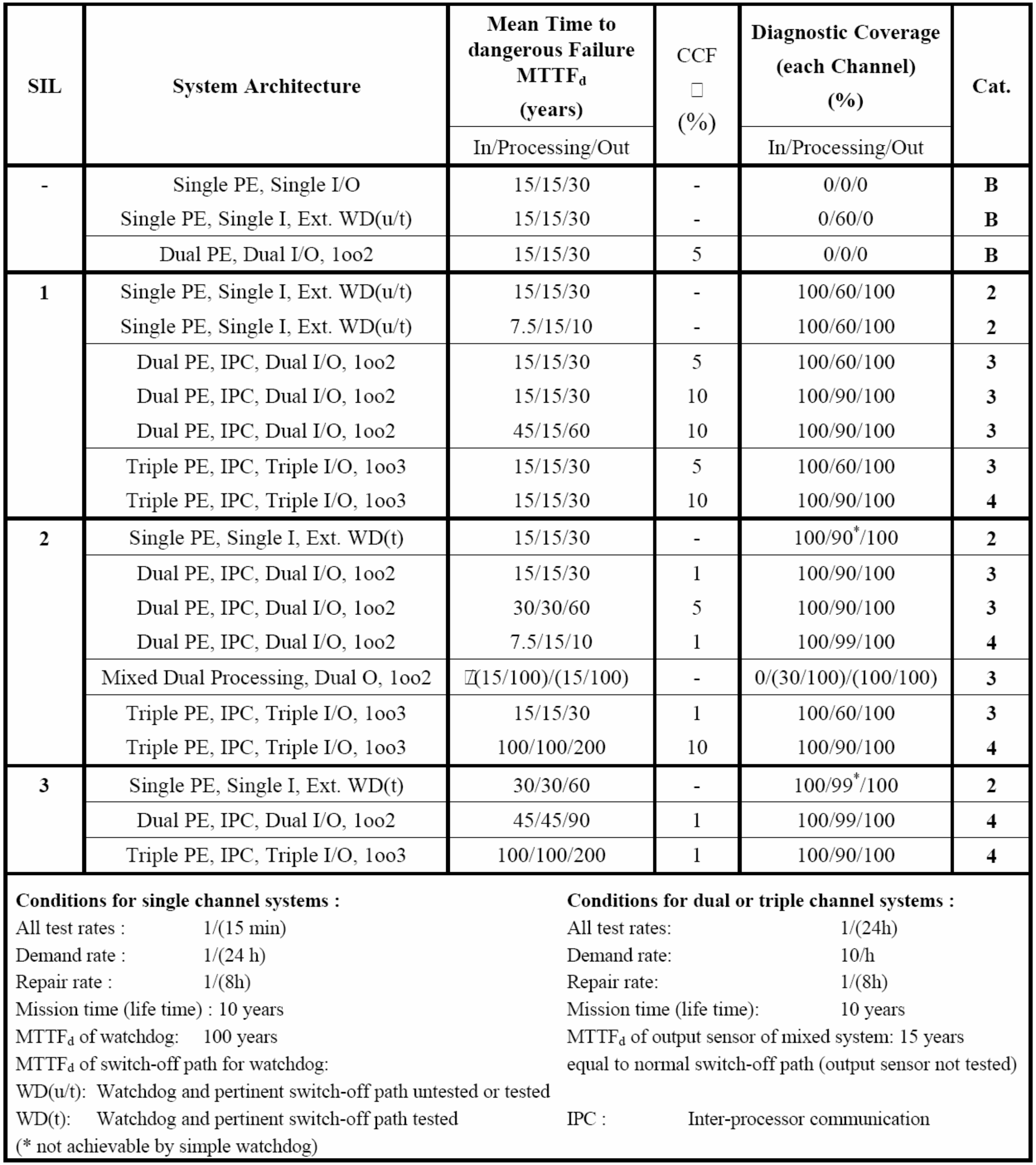


Comparison of Architectures used in Machinery Industry



Comparison of architectures from STARCES

Attempt to reconcile IEC61508 and machine standard EN954



SIL	System Architecture	Mean Time to dangerous Failure $MTTF_d$ (years)	CCF □ (%)	Diagnostic Coverage (each Channel) (%)	Cat.
		In/Processing/Out		In/Processing/Out	
-	Single PE, Single I/O	15/15/30	-	0/0/0	**B**
	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	0/60/0	**B**
	Dual PE, Dual I/O, 1oo2	15/15/30	5	0/0/0	**B**
1	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	100/60/100	**2**
	Single PE, Single I, Ext. WD(u/t)	7.5/15/10	-	100/60/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	5	100/60/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	10	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	45/15/60	10	100/90/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	5	100/60/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	10	100/90/100	**4**
2	Single PE, Single I, Ext. WD(t)	15/15/30	-	100/90*/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	1	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	30/30/60	5	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	7.5/15/10	1	100/99/100	**4**
	Mixed Dual Processing, Dual O, 1oo2	□(15/100)/(15/100)	-	0/(30/100)/(100/100)	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	1	100/60/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	10	100/90/100	**4**
3	Single PE, Single I, Ext. WD(t)	30/30/60	-	100/99*/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	45/45/90	1	100/99/100	**4**
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	1	100/90/100	**4**

Conditions for single channel systems :

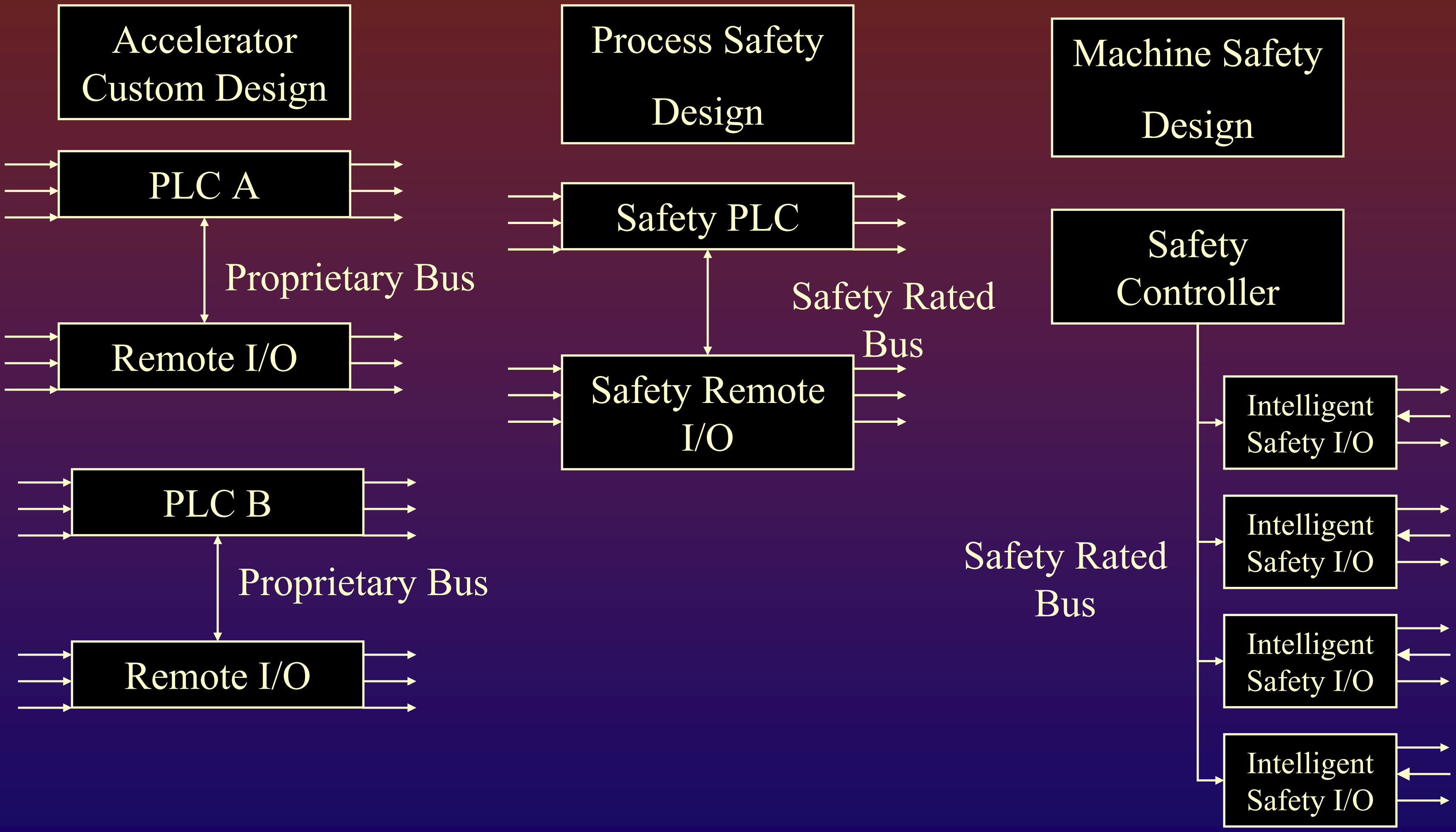
All test rates : 1/(15 min)
Demand rate : 1/(24 h)
Repair rate : 1/(8h)
Mission time (life time) : 10 years
$MTTF_d$ of watchdog: 100 years
$MTTF_d$ of switch-off path for watchdog:
WD(u/t): Watchdog and pertinent switch-off path untested or tested
WD(t): Watchdog and pertinent switch-off path tested
(* not achievable by simple watchdog)

Conditions for dual or triple channel systems :

All test rates: 1/(24h)
Demand rate: 10/h
Repair rate: 1/(8h)
Mission time (life time): 10 years
$MTTF_d$ of output sensor of mixed system: 15 years
equal to normal switch-off path (output sensor not tested)
IPC : Inter-processor communication

STSARCES
Standards for Safety Related Complex Electronic Systems

Sample Architectures for SIL 2/3


Accelerator Custom Design

PLC A

Proprietary Bus

Remote I/O

PLC B

Proprietary Bus

Remote I/O

Process Safety Design

Safety PLC

Safety Rated Bus

Safety Remote I/O

Machine Safety Design

Safety Controller

Safety Rated Bus

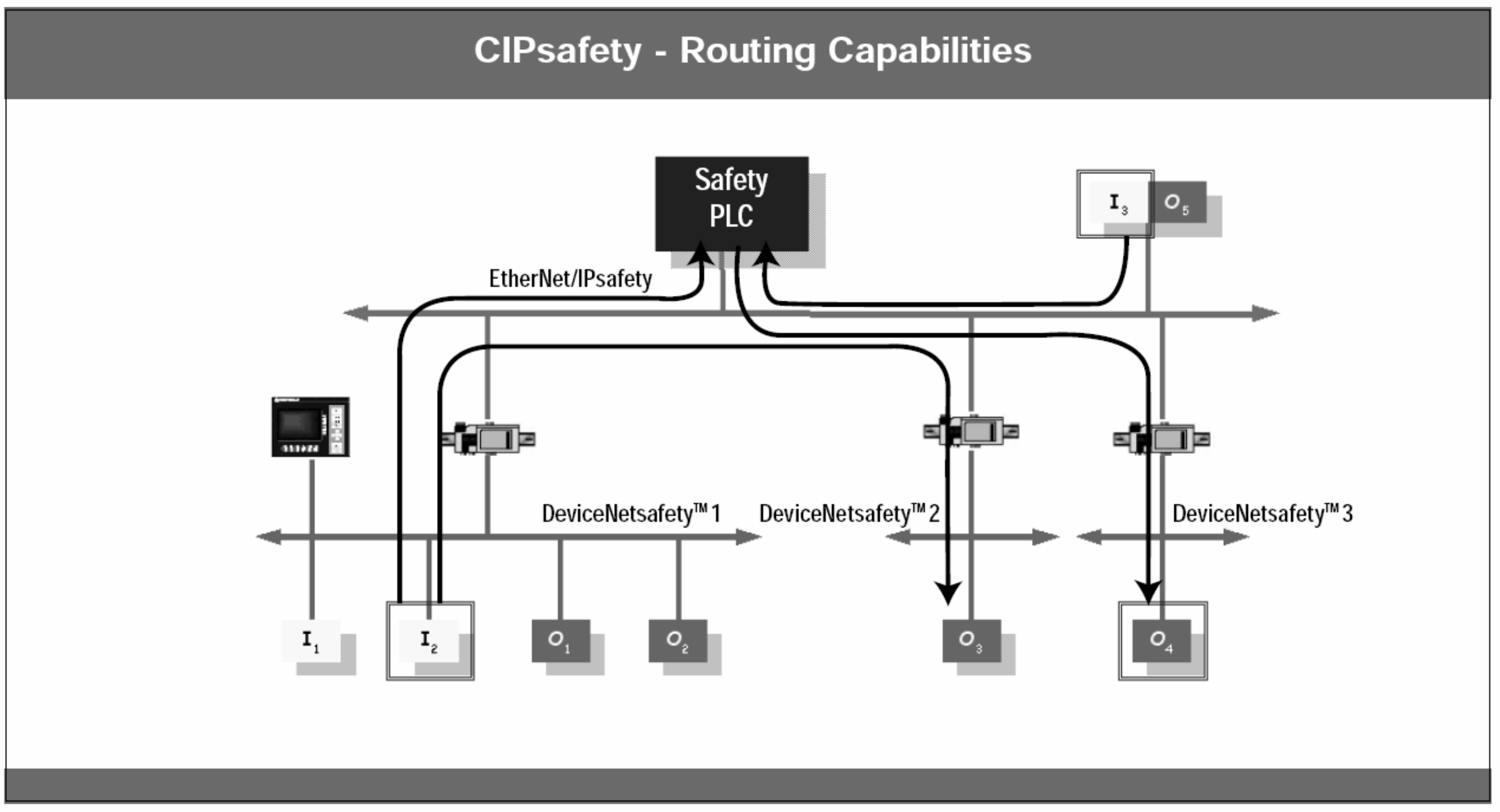
Intelligent Safety I/O

Intelligent Safety I/O

Intelligent Safety I/O

Intelligent Safety I/O

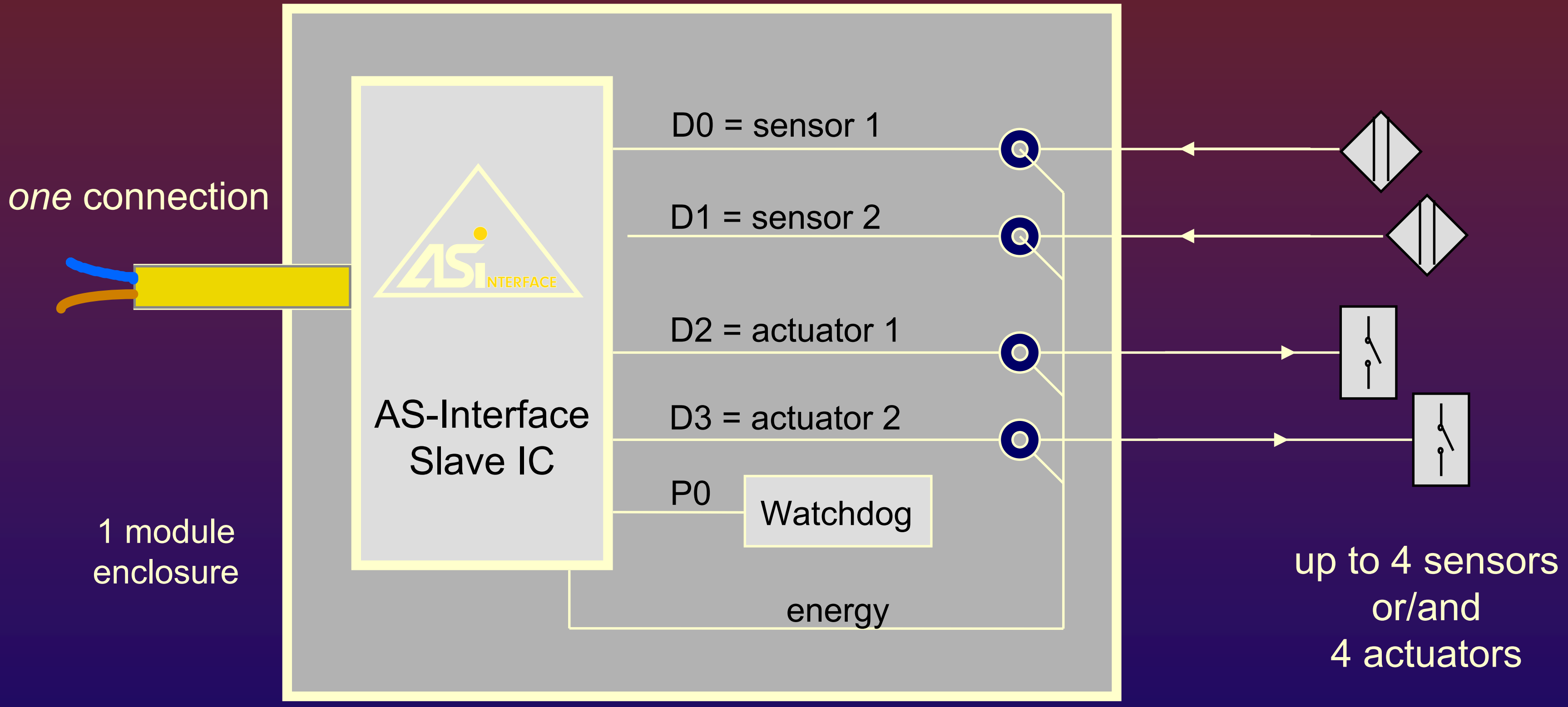
CIP Safety Net



CIPsafety - Routing Capabilities

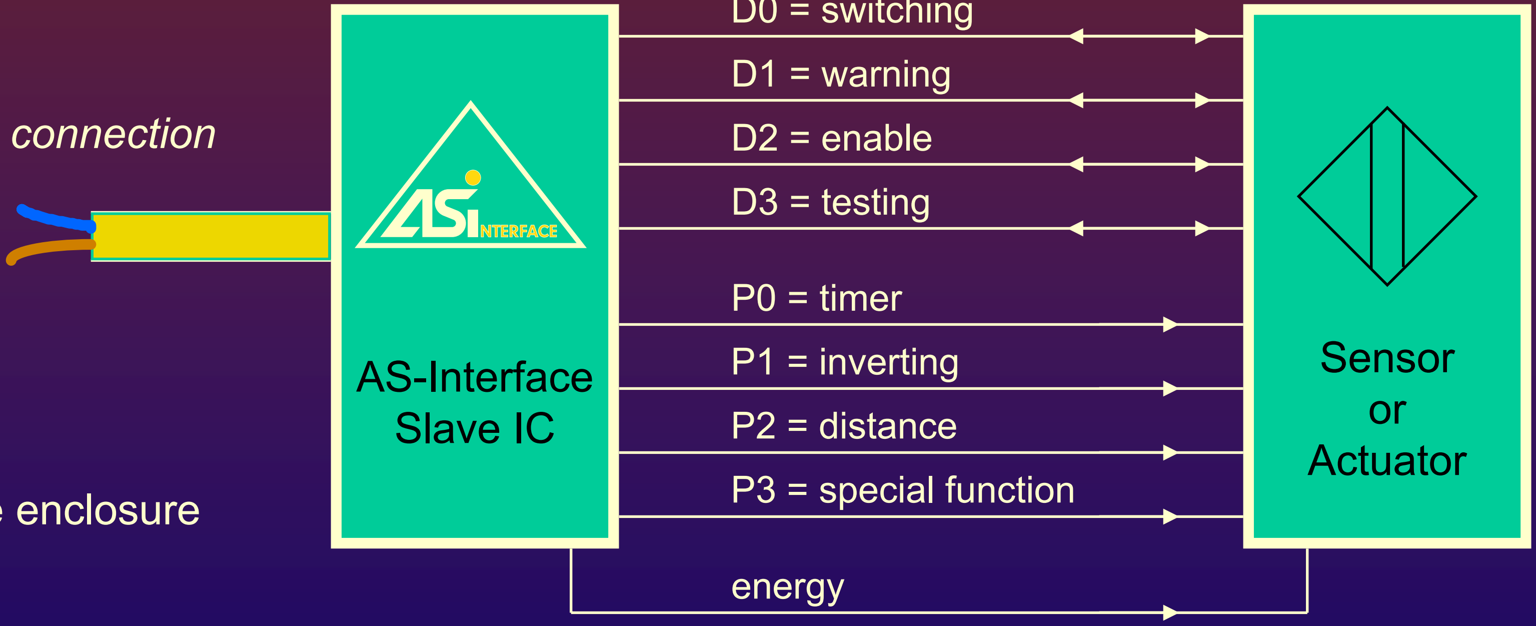
CIP=Common Industrial Protocol

Actuator Sensor Interface



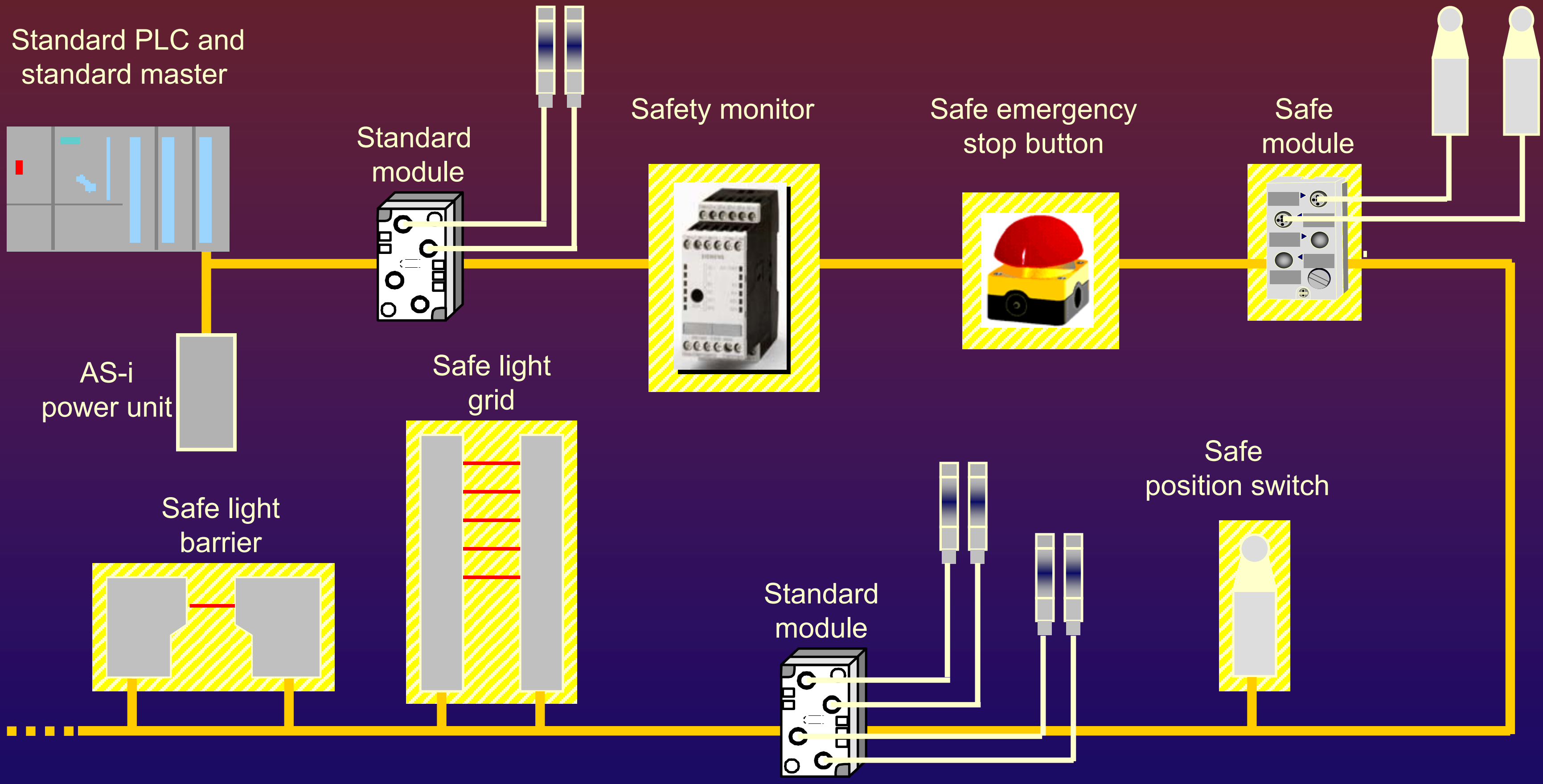
Courtesy of ASI International Foundation *one connection*

one enclosure



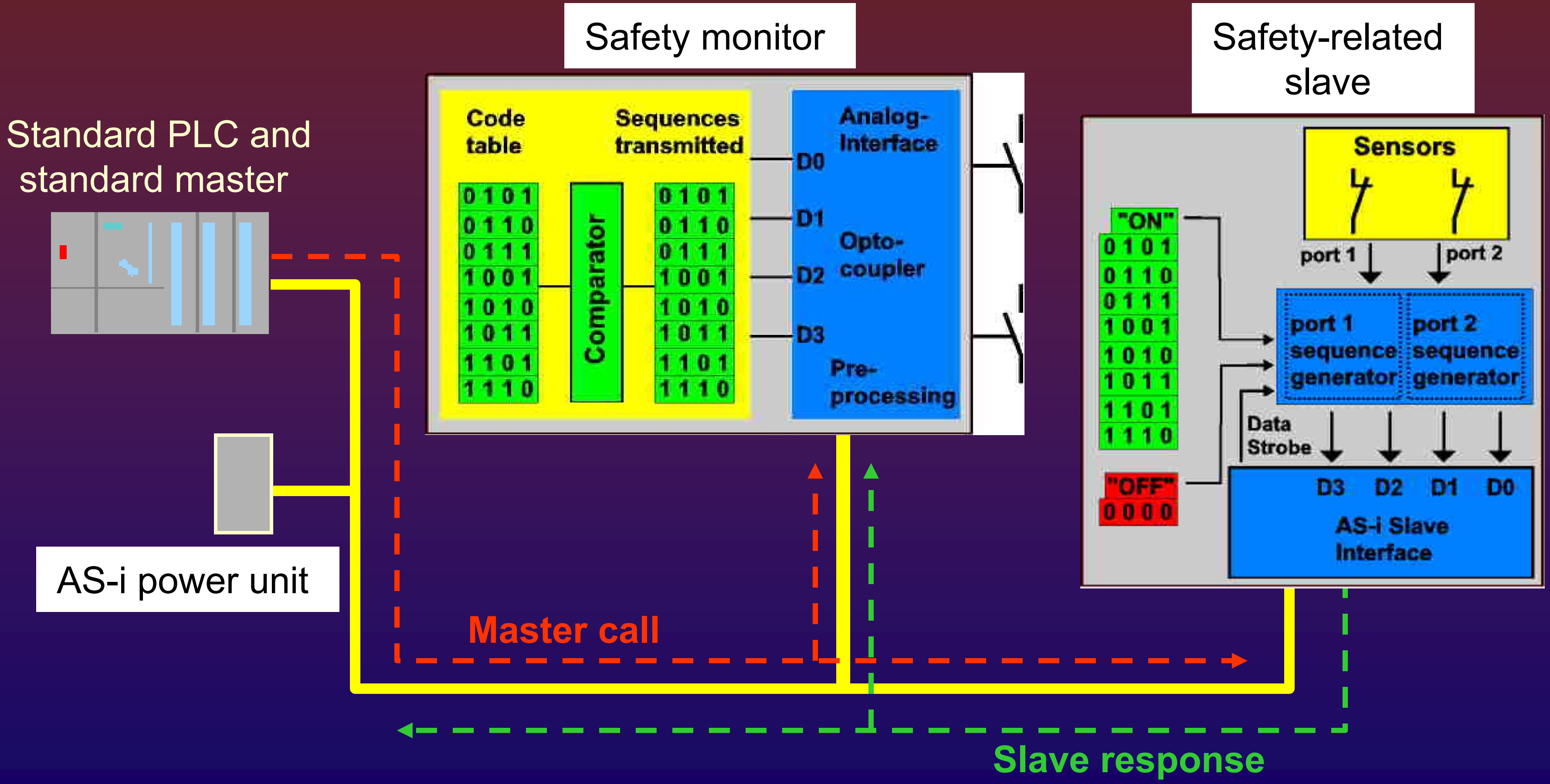
Courtesy of ASI International Foundation

ASI-Safety



© K Mahoney/S. Prior
2002-2004

USPAS
June, 2004



Safety monitor

Code table

0101
0110
0111
1001
1010
1011
1101
1110

Comparator

Sequences transmitted

0101
0110
0111
1001
1010
1011
1101
1110

D0

D1

D2

D3

Analog-Interface

Opto-coupler

Pre-processing

Safety-related slave

Sensors

port 1

port 2

"ON"

0101
0110
0111
1001
1010
1011
1101
1110

"OFF"

0000

port 1 sequence generator

port 2 sequence generator

Data Strobe

D3 D2 D1 D0

AS-i Slave Interface

Standard PLC and standard master

AS-i power unit

Master call

Slave response

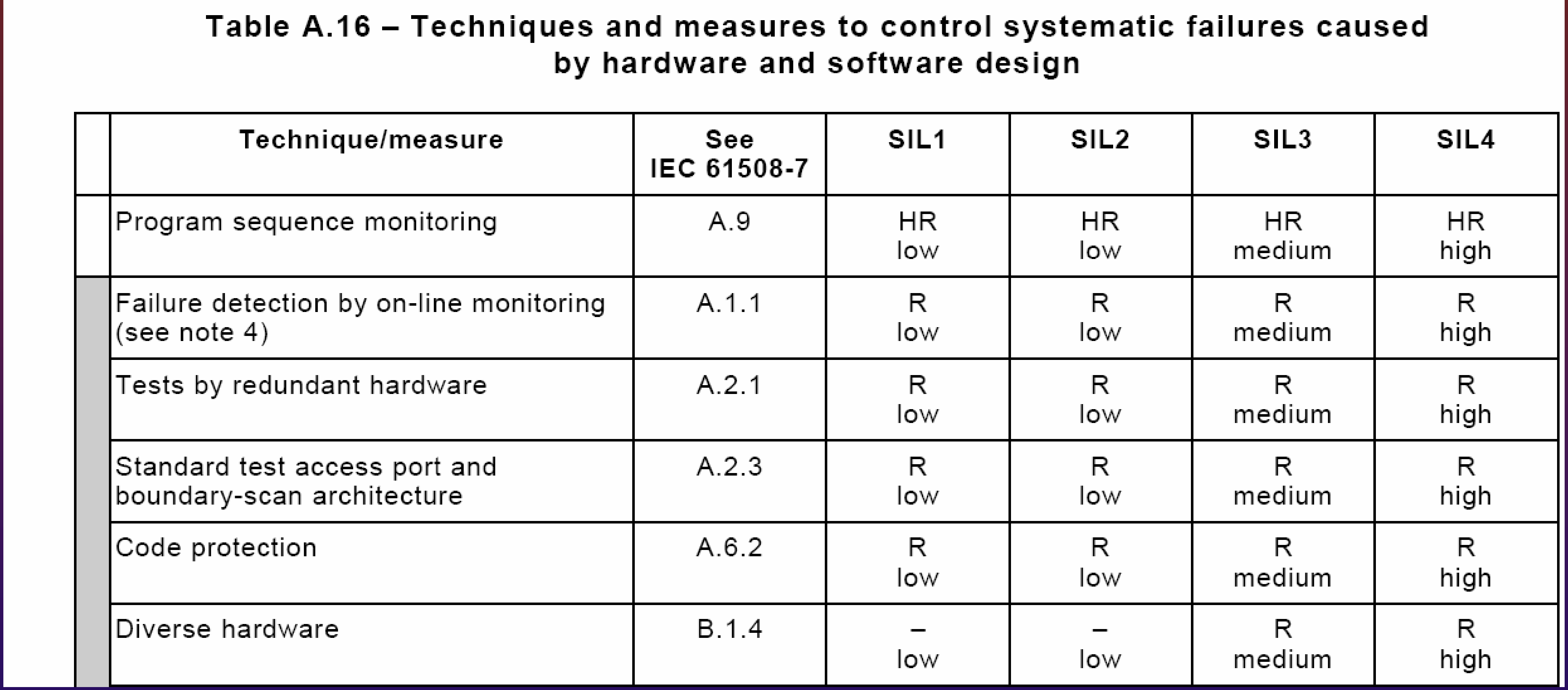


Table A.16 – Techniques and measures to control systematic failures caused by hardware and software design

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Diverse hardware	B.1.4	– low	– low	R medium	R high

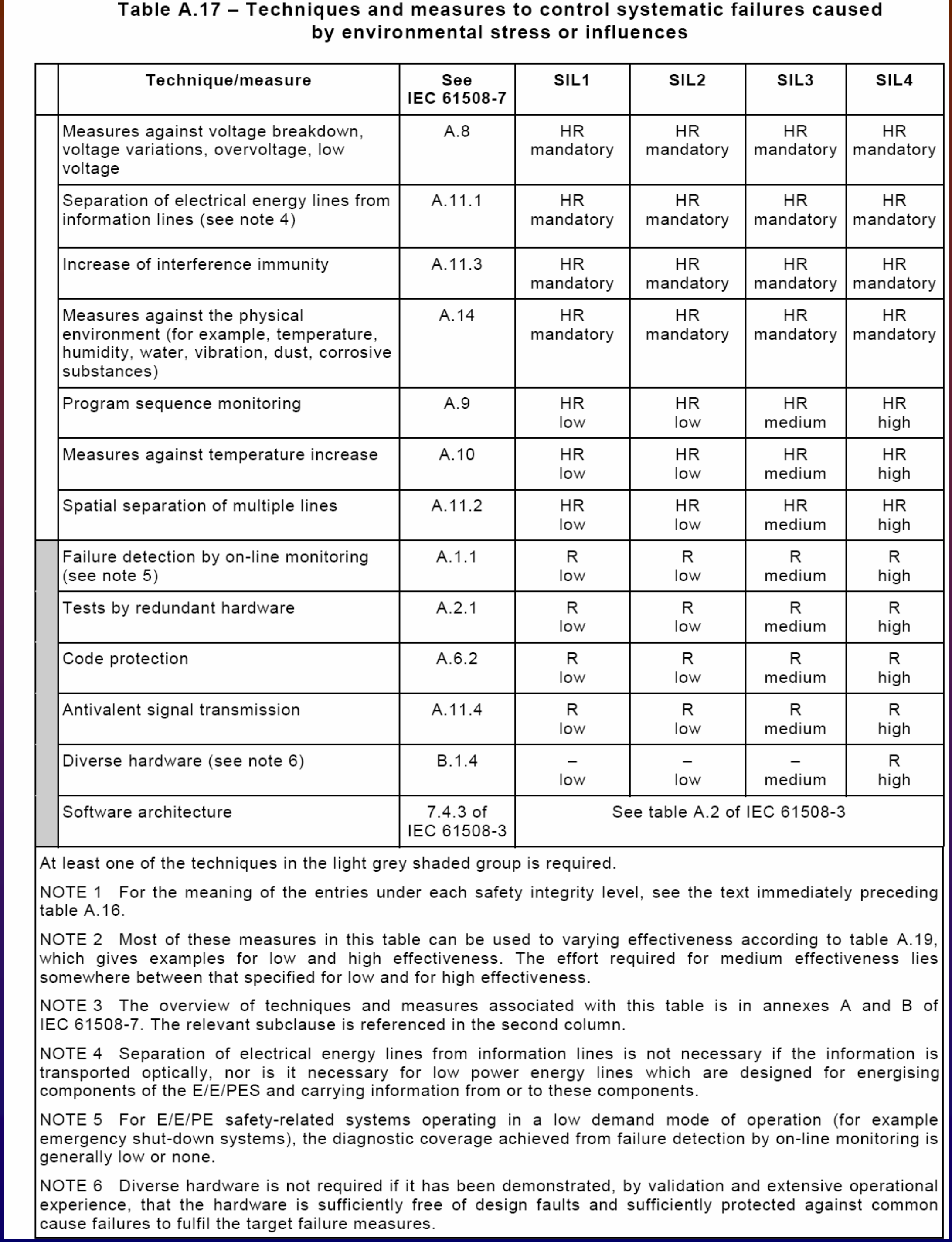


Table A.17 – Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage	A.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Separation of electrical energy lines from information lines (see note 4)	A.11.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Increase of interference immunity	A.11.3	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
	Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
▨	Failure detection by on-line monitoring (see note 5)	A.1.1	R low	R low	R medium	R high
▨	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
▨	Code protection	A.6.2	R low	R low	R medium	R high
▨	Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
▨	Diverse hardware (see note 6)	B.1.4	– low	– low	– medium	R high
▨	Software architecture	7.4.3 of IEC 61508-3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A and B of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 Separation of electrical energy lines from information lines is not necessary if the information is transported optically, nor is it necessary for low power energy lines which are designed for energising components of the E/E/PES and carrying information from or to these components.

NOTE 5 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

NOTE 6 Diverse hardware is not required if it has been demonstrated, by validation and extensive operational experience, that the hardware is sufficiently free of design faults and sufficiently protected against common cause failures to fulfil the target failure measures.

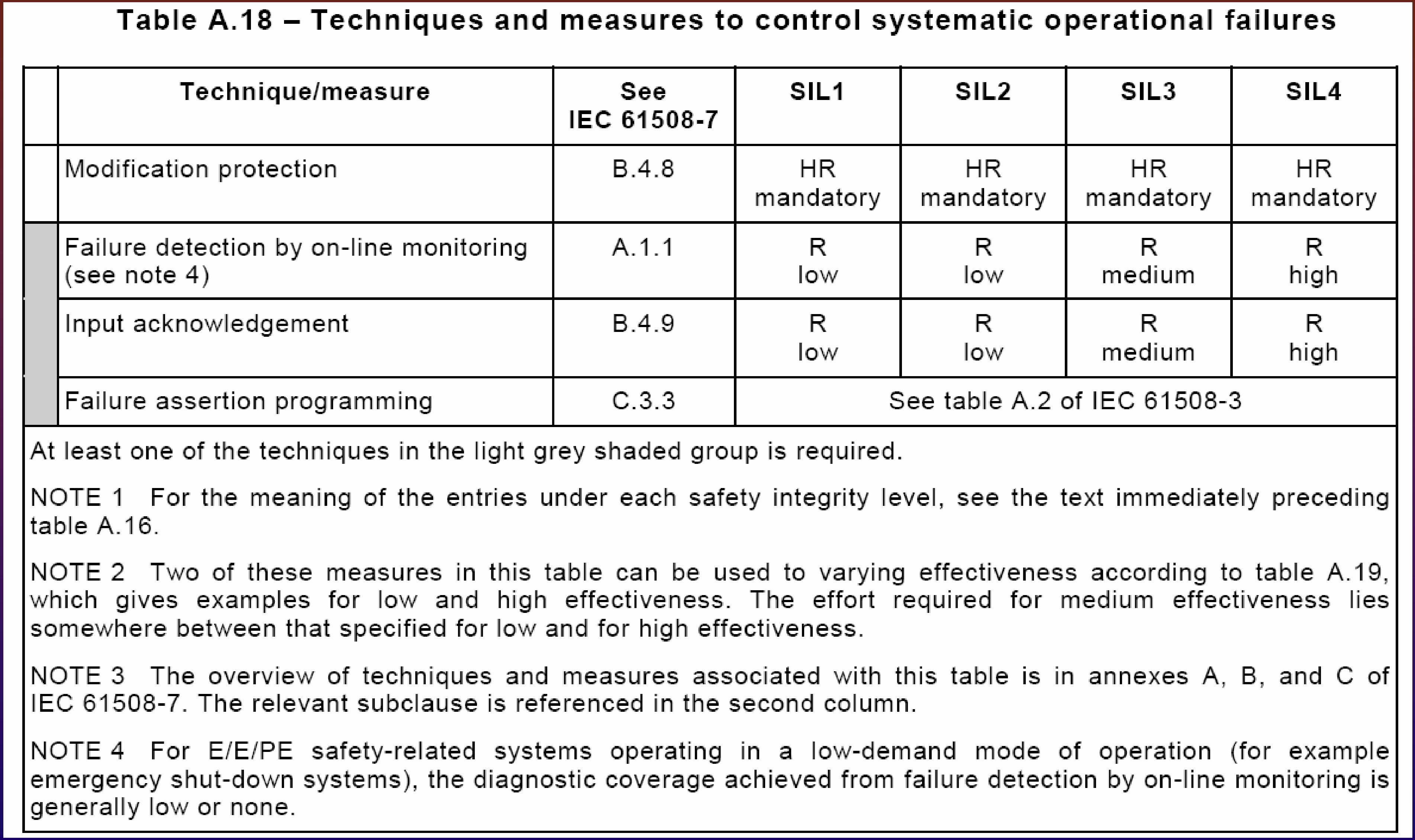


Table A.18 – Techniques and measures to control systematic operational failures

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Modification protection	B.4.8	HR mandatory	HR mandatory	HR mandatory	HR mandatory
▨	Failure detection by on-line monitoring (see note 4)	A.1.1	R low	R low	R medium	R high
▨	Input acknowledgement	B.4.9	R low	R low	R medium	R high
▨	Failure assertion programming	C.3.3	See table A.2 of IEC 61508-3			

At least one of the techniques in the light grey shaded group is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding table A.16.

NOTE 2 Two of these measures in this table can be used to varying effectiveness according to table A.19, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in annexes A, B, and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low-demand mode of operation (for example emergency shut-down systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.